CLAIMS:

1. (Currently amended) A method, comprising:

determining security information associated with ~~at least one~~ a object of a transaction, wherein the security information is inserted in a header of the object and the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device;

determining, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, ~~if an adjacent intermediate~~ whether a next device in the transmission path to which the object is to be transmitted ~~is adapted to provide~~ provides a level of security indicated by at least a portion of the security information in the header of the object; and

transmitting, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, the object to the ~~adjacent intermediate~~ next device in the transmission path in response to determining that the ~~adjacent intermediate~~ next device ~~is adapted to provide~~ provides the level of security required by the at least a portion of the security information.

2. (Currently amended) The method of claim 1, wherein the object is a business object, and wherein determining if the ~~adjacent intermediate~~ next device in the transmission path ~~is adapted to provide~~ provides the level of security comprises:

transmitting to the ~~adjacent intermediate~~ next device in the transmission path information representative of the level of security that is desired; and

receiving a response from the ~~adjacent intermediate~~ next device in the transmission path indicating that the ~~adjacent intermediate~~ next device in the transmission path ~~is adapted to provide~~ provides the desired level of security.

3. (Currently amended) The method of claim 1, wherein determining the security information comprises accessing [[a]] the header portion of the object;

wherein determining if ~~an adjacent intermediate~~ the next device in the transmission path ~~is adapted to provide~~ provides a level of security indicated comprises performing at least one of:

transmitting information representative of the level of security that is desired to the ~~adjacent intermediate~~ next device in the transmission path prompts the ~~adjacent intermediate~~ next device in the transmission path to execute at least one module that allows the ~~adjacent intermediate~~ next device in the transmission path to provide the level of security; and

comparing the ~~adjacent intermediate~~ next device in the transmission path to a list of trusted devices in the header portion of the object;

wherein the transmitting the object to the ~~adjacent intermediate~~ next device in the transmission path comprises transmitting the object to an object handler module in the ~~adjacent intermediate~~ next device in the transmission path;

wherein the object handler module is a business integration adapter supporting connectivity options, the connectivity options comprising at least one of packaged applications, custom applications, legacy applications, databases, trading partners' systems, and public information stores on the internet;

wherein the object handler module supports at least one of event-driven real-time synchronous connections, asynchronous loosely coupled connections with trading partners, synchronous on-demand connections to customers and synchronous tightly coupled connections to trusted trading partners;

wherein the object handler module includes at least one of a module for accessing the security information associated with a given object and a module for requesting the adjacent intermediate device in the transmission path to provide information about its security capabilities.

4. (Currently amended) The method of claim [[3]] 1, wherein determining the security information comprises determining security information relating to at least one of connection information, class information, trusted entities information, and logging capability information.

5. (Original) The method of claim 3, wherein accessing the header portion of the object comprises accessing at least one header of a Simple Object Access Protocol message.

6. (Currently amended) The method of claim 1, further comprising determining an alternative ~~intermediate~~ device along a different transmission path that ~~is adapted to provide~~ provides the level of security ~~represented~~ required by the at least a portion of the security information in response to determining that the ~~adjacent intermediate~~ next device in the transmission path [[is]] does not ~~adapted to~~ provide the level of security required by the at least a portion of the security information.

7. (Currently amended) The method of claim 1, further comprising sending a message to the ~~adjacent intermediate~~ next device in the transmission path instructing the ~~adjacent intermediate~~ next device to execute at least one module that allows the ~~adjacent intermediate~~ next device to provide the level of security required by the at least a portion of the security information.

8. (Currently amended) The method of claim 1, wherein determining the security information comprises determining the security information in response to receiving the object from at least one of a previous ~~remote~~ device [[and]] or a source device in the transmission path.

9-27. (Cancelled)

28. (Currently amended) A method, comprising:

receiving, at a first device along a transmission path from a source device to a target device, a request from a second device along the transmission path desiring to transmit ~~at least one~~ an object to a third device, wherein the request includes at least a portion of security information associated with the object, the portion of security information being provided in a header of the object;

determining if the first device is adapted to provide a level of security ~~represented~~ identified by the at least a portion of security ~~parameter~~ information in the header of the object; and

transmitting an indication to the second device, based on determining if the first device ~~is adapted to provide~~ provides the level of security identified by the at least a portion of security information; and

receiving, in the first device, the object from the second device only in response to the first device transmitting an indication that the first device provides the level of security identified by the at least a portion of security information.

29. (Currently amended) The method of claim 28, further comprising configuring the first device with at least one module that ~~allows the first device the adaptability for providing~~ provides the level of security.

30. (Cancelled)

31. (Currently amended) The method of claim 1, wherein at least one intermediate device includes at least a first intermediate device and a second intermediate device;

wherein determining if ~~an adjacent intermediate~~ a next device in the transmission path ~~is adapted to provide~~ provides a level of security required by the at least a portion of security information includes performing the determining at the source device, wherein the ~~adjacent intermediate~~ next device is the first intermediate device;

wherein transmitting the object to the ~~adjacent intermediate~~ next device comprises transmitting the object to the first intermediate device, and wherein in response to determining that the ~~adjacent intermediate~~ next device ~~is adapted to provide~~ provides the level of security ~~comprises~~, and in response to determining that the first intermediate device ~~is adapted to provide~~ provides the level of security~~;~~

~~further comprising~~:

determining, at the first device, if a second device of the plurality of intermediate devices that is adjacent the first device ~~is adapted to~~

~~provide~~ provides the level of security indicated by the at least a portion of the security information;

transmitting the object to the second device of the plurality of intermediate devices in response to determining that the second device ~~is adapted to provide~~ provides the level of security; and

transmitting the object to the target device from the second device.

32. (Currently amended) The method of claim 31, further comprising determining an alternative intermediate device along a different transmission path that ~~is adapted to provide~~ provides the level of security represented in response to determining that at least one of the first intermediate device and the second intermediate device in the transmission path [[is]] does not ~~adapted to~~ provide the level of security.

33. (Currently amended) The method of claim 1, wherein the at least one intermediate device includes a plurality of intermediate devices;

wherein determining if ~~an adjacent intermediate~~ a next device in the transmission path ~~is adapted to provide~~ provides a level of security comprises determining, at a previous device in the transmission path, a security level for each intermediate device of the plurality of intermediate devices;

wherein transmitting the object to the ~~adjacent intermediate~~ next device in the transmission path, in response to determining that the ~~adjacent intermediate~~ next device is adapted to provide the level of security, comprises transmitting the object to each of the plurality of intermediate devices in the transmission path in response to determining that each of the plurality of intermediate devices ~~is adapted to provide~~ provides the level of security;

further comprising:

transmitting the object to the target device.

34. (New) The method of claim 1, wherein the object is one of a plurality of objects of the transaction, and wherein at least two of the objects in the plurality of objects have different security information in their respective headers identifying different levels of

security required to be provided by devices along corresponding transmission paths to receive the at least two objects.